# NHIN Workgroup
# Draft Transcript
# April 14, 2010

## Presentation

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Thank you so much. Good morning, everybody, and welcome to the NHIN Workgroup call. This is a federal advisory committee, so there will be opportunity at the close of the call for the public to make comments. Let me do a roll call, please. David Lansky?

**David Lansky – Pacific Business Group on Health – President & CEO**
Yes.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Neil Calman?

**Neil Calman - Institute for Family Health - President & Cofounder**
Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Jim Borland?

**Justine Pierman – SSA – Senior Advisor Health Information Technology**
This is Justine Pierman for Jim Borland.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Thanks, Justine. Christine Bechtel? Tim Cromwell?

**Tim Cromwell – VHA – Director of Standards & Interoperability**
Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Marc Probst? Marc Overhage? Wes Rishel? Micky Tripathi? Colin Evans? Arien Malec? Jonah Frohlich?

**Arien Malec – RelayHealth – VP, Product Management**
I'm here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Arien is there. Jonah Frohlich?

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
Yes, I'm here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Carol Diamond?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Leslie Harris?

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
John Blair?

**John Blair – Tacanic IPA – President & CEO**
Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Farzad Mostashari?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Todd Park? Doug Fridsma? Deven McGraw?

**Deven McGraw - Center for Democracy & Technology – Director**
Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Mark Frisse? Andrew McLaughlin? Latanya Sweeney? Connie Delaney? Adam Green?

**Adam Green – Progressive Chain Campaign Committee – Cofounder**
Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Did I leave anybody off? All right. With that, I'll turn it over to David Lansky.

**David Lansky – Pacific Business Group on Health – President & CEO**
Thank you, Judy. Thanks, everybody, for making time for another discussion on the NHIN work. I appreciate everyone making time. I know everyone is swamped with health IT policy and technical work these days, so thank you for having time to join us. Our agenda today, hopefully you all received copies of the materials. We have an agenda we can go over quickly, and then we have a set of slides to look at. And the agenda has, as you see, two major topics for today.

One is to review the overall trust framework that we've spent some time in some small group discussions getting framed, and want to see if the committee as a whole is ready to bring this forward to the policy committee in a week or so. And the second topic is taking that trust framework in its initial layout and applying it to a couple scenarios, particularly the directed push of information that we think is required for the 2011 meaningful use criteria that we're aware of so far. And that will, in turn, raise some issues for some of the elements within the trust framework.

With that, let's just dive in. If you've got copies of the materials, we can start on slide three. And I think, because we've been over quite a bit of this material, we can probably review these elements fairly quickly. But if not, we'll stop and do what we need to do.

Slide three just reminds us of the February comments we made to the full policy committee that we believe we need to establish and make in a framework of trust, which insures adequate privacy and security protections for health information exchange, and then there are some principles underneath those that we've previously agreed upon. So today's discussion is on that first bullet looking at the trust framework.

The next slide, number four … that there is a need at the national level trust framework to enable information exchange, which will be a tool to understand how trust can be implemented across a range of uses and scenarios. And we're going to start with the 2011 meaningful use criteria, but we're not going to be limited by that. We will address privacy and security issues.

We will articulate the comment elements that are needed for exchange partners to … health information exchange. And we have, in our discussions, noted that this framework, as it is implemented, will vary depending on a variety of factors, types of exchanges occurring, types of partners involved in exchange, and so on. We also, of course, want to enable interoperability from a policy and the policies in place to support interoperability, and we want to take advantage of your experience and others with HIE already.

Continue to the next slide, and then we'll look at these together. We noted that the perceived value of an exchange creates incentives for all the parties to comply with the trust framework. We all recognize that ultimately participation in this exchange is voluntary, that value creates an incentive to abide by, continue to comply with the trust requirements to keep getting that value from the exchange. And knowing that the other partners in the exchange also derive value from it, provide some assurance for continued compliance. This is really just an observation that underlies some of the approach we're taking to implementation of NHIN policy.

Let me stop on those two slides, four and, and just see if there are any concerns, comments, if people are comfortable moving ahead with those findings, as stated. Hearing no objection, we'll proceed with slide six.

Now here we've essentially taken concepts that were presented at the policy committee meeting last time, and we've done some reworking of the language, as we were encouraged to do, and some rebundling o the concepts that were in the, I think, six categories of framework elements that we described at the policy committee meeting had been regrouped and renamed. Otherwise, this should be content that is familiar, but I would like us to approve it if we can today to take it forward. So this now has five elements in the overarching trust framework, agreed upon business policy and legal requirements, transparent oversight, accountability and enforcement, the identity and authentication work, and then a set of minimum technical requirements. The next several slides lay those out in a little more detail. Hopefully today we can see if we can come to rest on these five descriptions.

Slide seven has a slightly longer description of….

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**

….

**David Lansky – Pacific Business Group on Health – President & CEO**

Yes?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
This is Farzad. I just want to mention two things, if I may.

**David Lansky – Pacific Business Group on Health – President & CEO**
Please.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
The first is that as folks will see, this is meant to be very kind of high level and general, and then we will next cone down on the implications for the more simple exchanges that we've been considering as part of this workgroup. The second is just to add on the previous slide, in kind of the plain English way for me, what made a lot of sense was that if you know that – you know that you derive value, and your partner derives value from the exchange, and that there's an expectation that you're going to be, both going to be in this.

This is not just a one-time transaction. That there is, I think the other aspect to this is the kind of like the prisoner dilemma game. If you do multiple trials, people's rational actions are different than if it's a one-time trial. So the expectation that if you screw up, you'll lose something of value over the long-run is, I think, another consideration.

**David Lansky – Pacific Business Group on Health – President & CEO**
Do you think that the last bullet point on slide five should be made more explicit on that point that the long-term, persistent value of the relationship is something that--?

**Aneesh Chopra – White House – CTO**
Either long-term or repeated contributes to that. I don't know how other folks feel about that.

**David Lansky – Pacific Business Group on Health – President & CEO**
I'm sure it's true. I wonder, though, whether it raises the flip side of the concern, which is, are people going to be – is it a different set of expectations or criteria for those engaged in what they perceive to be a one shot relationship … with a remote partner, etc.? They don't really have a local infrastructure that gives them value, but they're on the receiving end, let's say, of an occasional exchange at this early stage of the network development. I don't know. We're not saying this is a precondition or a necessary condition for having trust in the – being a recurring partner with others isn't a precondition of being, setting trust in the network or trust in the exchange. Any other reactions on that last point?

**Neil Calman - Institute for Family Health - President & Cofounder**
Yes. This is Neil. I guess, as an adjunct, it's fine, but one of the issues is that the people who gained value aren't necessarily the ones who are going to breach the trust, so in an organization that gains value from participating in exchange, you know, that doesn't really provide any assurance or protection at all that people within that organization, you know, a nurse, a clerk, or somebody else is not going to breach the trust of the patients and, you know, misuse information. I guess I'm feeling like it's sort of a weak bond because the benefits don't always match the places where trust might likely be violated.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. This is Deven. I think some of this accountability stresses a little too much of sort of a voluntary aspect in some sense that it's in your better interest to comply versus the points that I think Neil raised in some instances that may not be the case. And so I know we've talked about and will talk about sort of governance issues, and there's lots of detail that we need to put, that we still need to discuss. I'm wondering if some of the language here needs to be open to models of accountability that are both about

voluntary participation and perceived benefit and also accountability for compliance with policy that is overseen by someone other than the participant, to which there are consequences.

**David Lansky – Pacific Business Group on Health – President & CEO**
Yes, I think that's true. It's a hopeful element on slide five, but it doesn't have the balance of the public interest accountability on that particular statement.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Neil Calman - Institute for Family Health - President & Cofounder**
And I think the danger in that is that people read this, you know, and without knowing the full scope of spectrum of the things that we're going to really rely on, not that we're not going to really rely on this too, but that it's just, it sounds, it softens the whole picture. That's all. Anyway, I don't….

**David Lansky – Pacific Business Group on Health – President & CEO**
And I think Carol Diamond made the point earlier that none of these are all or one, and they work, you know, nothing in isolation is sufficient, and these really all work together to promote trust, which is, again, not an absolute, and that's also a spectrum, but points well taken.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. I mean, I think that's right, but I'm just looking back on a different slide about even the accountability and enforcement language. Each participant must accept responsibility for it's exchange activities and answer for adverse consequences. It's soft. There's kind of a missing, you know, each participant must be held accountable.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Right, comply with law, rules, regulations, governance.

**David Lansky – Pacific Business Group on Health – President & CEO**
Let's get to slide seven.

**W**
Did we skip one? Maybe not.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. No, okay, so it's slide 11 on our screen. It's in my paper deck.

**W**
Yes.

**David Lansky – Pacific Business Group on Health – President & CEO**
Yes, the slide number three, accountability and enforcement is where you want to draw attention?

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**David Lansky – Pacific Business Group on Health – President & CEO**
So we're going to come back to that, but it sounds like the point well taken, and I guess what I'd ask the group is whether on slide five where Farzad started us, we want to add a full bullet that mirrors the first

one, which emphasizes voluntary appreciation of the value with another bullet, which emphasizes this point of public interest, reasons to expect compliance with the trust framework.

**Deven McGraw - Center for Democracy & Technology – Director**
Right. You could call it public accountability.

**David Lansky – Pacific Business Group on Health – President & CEO**
I like the idea of saying that perceived value of exchange creates incentives to comply with trust framework. The public interest in the sets of this network and the protection of privacy and security also creates an incentive to … not only an incentive, but with an infrastructure for compliance or mechanisms for compliance.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**David Lansky – Pacific Business Group on Health – President & CEO**
Assurances to compliance.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
This is Leslie. I'm actually not sure I understand what that means.

**David Lansky – Pacific Business Group on Health – President & CEO**
The question, again, I guess is what are the reasons that any participants are going to comply with the trust framework. One we're saying is there's self interest, given a set of business incentives, in effect, or clinical incentives. And the second is they're going to comply with it because they have to. There are penalties and public….

**Leslie Harris – Center for Democracy & Technology – President & CEO**
That's less soft and, I think, a clearer way of saying it, better than there's public interest reasons.

**David Lansky – Pacific Business Group on Health – President & CEO**
Yes. Okay. Yes.

**Neil Calman - Institute for Family Health - President & Cofounder**
Actually, the word "incentive" makes it sound like it's voluntary. I mean, people think incentives are voluntary.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Yes, I agree.

**Neil Calman - Institute for Family Health - President & Cofounder**
And when you put that as sort of the heading, the whole thing kind of weakens. It's kind of like, oh, well, there are incentives for doing it, but there's not really a requirement to do it. Even though that's another bullet, I still think it's important to strengthen this.

**David Lansky – Pacific Business Group on Health – President & CEO**
Any suggestions how to do that, Neil? Do you want to change the word "incentive"?

**Neil Calman - Institute for Family Health - President & Cofounder**
Maybe to say--

**M**
Motivation.

**Neil Calman - Institute for Family Health - President & Cofounder**
--the state's requirements to comply with the trust framework.

**M**
How about motivation?

**Neil Calman - Institute for Family Health - President & Cofounder**
Motivation.

**W**
Well….

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
No, it should be….

**M**
My point, the reason I like having the mention of this is that it is important for people to be motivated to want to exchange information and to want to do it in a trustworthy way, and that's important.

**W**
Right, so the motivation may be here that motivating it to do right is what they have to do to achieve meaningful use. That I get.

**M**
But also their ongoing business relationships and their professional standards and so forth, it's not all about qualifying for the incentives.

**W**
Right.

**Deven McGraw - Center for Democracy & Technology – Director**
No.

**W**
And maybe we have to kind of lay that out a little bit more. Maybe it's just in its first, so it's sort of the first thing out there is very, very….

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. I mean, I kind of like the way David, you know, he said it in two ways, which maybe the language was less flowery, but it was quite direct, and I think it accurately captured what we were saying, which is, number one, yes. All of that … there are, there should be these other, what we might call soft incentives to participate. You should want to do this, and we should be setting up the trust framework that enables that, you know, those sort of incentives that we think ought to be there. But there's a second piece to this, which is, when you're there, you're going to have to comply with rules and be held accountable to them beyond your own individual incentives to be a professional and to do the right thing.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Right. I would say that it's fine to say that the value of exchange creates incentives to participate in health information sharing and the requirements to comply with a trust framework.

**Neil Calman - Institute for Family Health - President & Cofounder**
I like that.

**W**
I like that too, Carol, because the trust framework really isn't the soft incentives for this.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
No, the incentive is for health information sharing.

**W**
Right.

**Neil Calman - Institute for Family Health - President & Cofounder**
I like that.

**M**
Good idea.

**David Lansky – Pacific Business Group on Health – President & CEO**
All right. Done. Thank you, Farzad, for redirecting our attention. Let's review slide seven, the one in my deck is number seven, which is the five bullets on the trust framework with some explanatory text for each. We've already heard there may be some need to tighten number three, but let's go through them each. I wonder if we're better off going through each of the detailed slides and then coming back to the summary slide.

**Neil Calman - Institute for Family Health - President & Cofounder**
I would like that. Yes.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes, that's a good idea.

**David Lansky – Pacific Business Group on Health – President & CEO**
So let's start on the next slide numbered one, agreed upon business policy and legal requirements. There are two major points on this slide. We will need an agreed up on and mutually understood set of expectations, obligations policies, and rules around how partners will conduct their business generally and their exchange related activities specifically, not necessarily top down regulations. Assumes participants will adapt to the law. Requires participants to act in a way that protects privacy and security … with context. There need to be methods for confirming, detecting, and enforcing compliance. Let's pause on this slide and see if people feel like this is a sufficient explanation of the first element of the trust framework.

**M**
I mean, the trick here is not to make it so broad that it basically is the trust framework, and it encompasses accountability, redress, transparency, and everything else in this one bullet.

**M**

It's hard to hear you.

**Neil Calman - Institute for Family Health - President & Cofounder**
I'm not sure they're talking to us.

**David Lansky – Pacific Business Group on Health – President & CEO**
I think maybe someone should be on mute if they're having an outside conversation.

**M**
One of the discussion points here is that in order to trust sending information to someone or getting information from someone, you have to trust not only aspects of the exchange, but also what people do with the information within their organizations once it's been transmitted. I think it also gets to the point Neil brought up earlier. But we want to be careful not to get into kind of scope creep of the NHIN workgroup too much into that, but this is meant to convey that point as well that in order to trust the exchange, you've got to trust what people do with the information within their walls as well. And we're looking, just so people know, we're looking for the privacy and security workgroup to delve into that issue much more deeply in terms of what is required to insure privacy and security, basically pullet two here. You have to require participants to act in a way that protects privacy and security of the information once they've received it.

**Deven McGraw - Center for Democracy & Technology – Director**
Right, although presumably—this is Deven—once they've received it, they have a set of rules, both federal and state, that govern what they can do with that data and, similarly, maybe their own policies.

**W**
I assume we're talking about internal policies for handling data….

**Deven McGraw - Center for Democracy & Technology – Director**
Right. I mean, to some extent, if you know the person to whom you're sending the data, and the trust elements are sufficient that you have confidence that when you send the data to Dr. X, in fact, that is Dr. X, and she received it. What additional level of confidence is going to be needed to facilitate that exchange beyond some expectation that whatever they're doing with data is, you know, in compliance with law and whatever are the professional obligations.

**John Blair – Tacanic IPA – President & CEO**
Yes. This is John. I had the same question, Farzad. Doesn't current law handle it once it's…?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right. Maybe it does. Maybe it doesn't. All I'm saying is that to dig deeper into that is not us. It's the privacy and security workgroup, Deven, and I'm hoping you'll agree to that.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. No, no, yes. No, I don't disagree with that at all. In fact, I sort of look at these next series of slides as being more sort of top of the trees, here are the sort of big categories that a trust framework needs to hit without going into too much detail about what that would look like because I think you're right that there are other workgroups that are likely to flush some of that out and other pieces we would flush out here.

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**

This is Jonah. I do think it's important to note that we're talking about a common understanding … disclosures by all participants and that that will be flushed out by privacy and security, but that is a very critical component of the trust framework.

**David Lansky – Pacific Business Group on Health – President & CEO**
I like that phrasing better than business generally because it implies we're going to get into everybody's business. We're talking about uses and disclosures of health information.

**Neil Calman - Institute for Family Health - President & Cofounder**
I think what we're trying to say is that the special things that exchange requires really builds on top of the general framework that we're creating around health information privacy and security.

**David Lansky – Pacific Business Group on Health – President & CEO**
Right.

**W**
Yes, it doesn't … it doesn't quite say that.

**Neil Calman - Institute for Family Health - President & Cofounder**
Correct, but isn't that what we're trying to say is that it really sits on top of that.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. Absolutely. We're not giving providers any additional permissions to share data with entities that today they can't share data with. I mean, we already do, for better or for worse, have a set of laws, imperfect in many ways, but nevertheless, there's a code of conduct that does exist in law, and this should layer on top of it and address the issues that are not well covered.

**M**
Yes. Really interesting and, I think, informative examples of this was around identity assurance. I'll give a little sneak preview. Andrew McLaughlin, I don't think Andrew has joined us yet, has he?

**Judy Sparrow – Office of the National Coordinator – Executive Director**
No.

**M**
Is going to lead a little working group to start thinking through the level of identity assurance required in the context, right, as we heard the context makes all the difference. One of the first things we realized in doing this was you can't just look at the transaction to determine the level of assurance needed for the transaction because, as was raised in the testimony we heard, all the federal standards used for doing the risk assessment are assuming a remote access model. Whereas, if you're already in an electronic health record in an emergency department with a stethoscope around your neck behind the nurse's station, and you're already in the system, and you can change people's information and write them for an injection of whatever.

The added level of identity assurance needed to do now an electronic prescription may be nothing, right? So it matters what you're building on top of. And perhaps this is where we're going with the identity assurance thing. Perhaps to only talk about the level of identity assurance required for a transaction doesn't make sense unless we've already established the level of identity assurance required to get into the application, to get into that kind of health IT application in the first place, and then ask the question, is there anything more that we need for doing particular transactions once you're in the system.

Again, pointing out, as Neil expressed it, that this builds on top of the base of what has to happen for privacy and security of the uses of information. What's on top of that then becomes the issues around the exchange of information.

**David Lansky – Pacific Business Group on Health – President & CEO**
That would be a useful point to add to the context sub-bullet, either before it or after it, just building upon the broader set of accepted practices or enforced practices around privacy and security of information. I want to go back to Jonah's suggestion and ask whether in the first paragraph where the phrase "partners … conduct their business generally" could be replaced by "around uses and disclosures of health information", or will people feel that's too narrowly constructed? My suggestion was "agreed upon, mutually understood set of expectations, obligations, policies, and rules around uses and disclosures of health information".

**Neil Calman - Institute for Family Health - President & Cofounder**
I think that's too narrow, especially if you think about what Farzad just said. It also has to do with how people handle their passwords, how they handle their roles in terms of who has access to what types of information. I think there's a lot more than just that.

**M**
Yes. What Farzad said, this leverages the security and privacy aspects of the EHR, the edge application.

**M**
Yes.

**M**
It certainly needs to be considered in the context of that.

**M**
Yes.

**M**
But I do agree that conduct their business generally is a little too generally.

**Neil Calman - Institute for Family Health - President & Cofounder**
So maybe conduct, you know—

**M**
Protect health information?

**Neil Calman - Institute for Family Health - President & Cofounder**
Right, protect health information in general or something.

**M**
How about use, protect, and disclose health information?

**M**
Okay.

**Neil Calman - Institute for Family Health - President & Cofounder**

That's fine.

**David Lansky – Pacific Business Group on Health – President & CEO**
Other comments on this slide or amendments to it you'd like to propose? Do you want to try to capture, Farzad, the suggestion of the broader statement you made about building upon an existing mechanism in the set of sub-bullets, which is an analogous to the first one around compliance with law? Essentially this would be one to say builds upon.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
That could almost be the first bullet, the first sub-bullet.

**David Lansky – Pacific Business Group on Health – President & CEO**
Yes. People wanting to capture that thought here?

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**David Lansky – Pacific Business Group on Health – President & CEO**
Okay. We'll find a way to do that. Okay. Other comments on the slide as a whole?

**Deven McGraw - Center for Democracy & Technology – Director**
Maybe you were hinting at this earlier, David—this is Deven—that the methods for conforming to … and enforcing compliance, and I get why this looks like an agreed upon business policy and legal requirement, but shouldn't this be part of the accountability bucket?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes, that's where I was going early. I think maybe I would suggest removing this second….

**David Lansky – Pacific Business Group on Health – President & CEO**
Yes, I agree. If there are no … we'll do that, capture it in the next two. Okay. Last chance … leave it at that. Actually, while we're here, let's just go back to the original … previous slide, the trust framework slide, and see if now the summary that's shown here is still what we want to use for the high level summary. It now says all participants will abide by an agreed upon set of rules, including compliance with applicable law and act in any way that protects the privacy and security of the information.

**Neil Calman - Institute for Family Health - President & Cofounder**
I think it's good.

**David Lansky – Pacific Business Group on Health – President & CEO**
That sounds good to me.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes, that's fine.

**David Lansky – Pacific Business Group on Health – President & CEO**
Right. No objection, we'll go to the next bullet, transparent oversight. Oversight is intended to mean management, maintenance, supervision, and monitoring of the trust relationship and exchange activities. It should be as transparent as possible. For example, governmental oversight may not be entirely transparent. The nature of oversight and mechanisms used will depend upon exchange characteristics model and needs identified by exchange partners. For example, oversight could be provided by the

parties to the exchange, individual subjects of the exchange information … centralized oversight mechanisms third party governmental oversight.

**W**
Do we mean third parties like audits? What do we mean by third parties?

**David Lansky – Pacific Business Group on Health – President & CEO**
I think audits, so if we had an accreditation function, that could be triggered.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**W**
Yes.

**David Lansky – Pacific Business Group on Health – President & CEO**
I have a little trouble with the boundary between the oversight function and the enforcement function, especially those last couple points.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**W**
Yes, well, that's why I was asking because … auditing is about transparency, but auditing is also about compliance, and it may not be about transparency depending on what you ask the auditor to do.

**M**
Carol, you had been eloquent about arguing for this. Can you rephrase what you were talking about in terms of the transparency requirement apart from compliance?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Yes. I was arguing for two levels of transparency. One is the transparency in the context that we've been discussing it, which is, people know what is happening with their information, put simply. The other level of transparency I was arguing for was transparency in the oversight. In other words, whatever the oversight mechanism is that people have an opportunity to understand the findings of that oversight and the consequences of that oversight and the mechanisms of that oversight.

**David Lansky – Pacific Business Group on Health – President & CEO**
Would it make sense to put it after compliance so that we first hear about what accountability enforcement is and then talk about the need to be transparent in the conduct of that?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Sure. The point is really that whatever the oversight mechanism is that it be visible to the participants and to potential users so that if there's a finding in that oversight that it be immediately visible.

**Neil Calman - Institute for Family Health - President & Cofounder**
This is Neil. Can I just – I guess I still have this sort of concern that we're creating something that doesn't, that's not possible to really look at on an individual level. Like, you know, if there's a mass release of information or somebody hacks into a computer system or whatever, you know, we've had six breaches so far: two on exchange, one this week, and four through our regular electronic health record, and not

one of them would be picked up by any kind of mechanism of audit or anything else, especially on the exchange. Once the information is transferred from one organization to another, the sending organization has no way of auditing the further release of that information in the second organization: who is talking to whom about it, where that information gets left, what happens with it.

I mean, I think people need to … I guess I'm supporting what Carol is saying, but in a different way. People need to also know what the limitations are of our ability to secure their information because it has real limitations, even in the most aggressive of oversight circumstances. We can't really secure their information.

**M**
…from there I understand….

**Neil Calman - Institute for Family Health - President & Cofounder**
Part of my transparency would be the way we do informed consent. You don't just tell people all the good things that are going to happen, but there needs to be a real understanding on people's point so that they can make an appropriate assessment about the risks of the information that they're sharing in their consent. And they need to know that there are limitations to the ability for us to protect their information, specifically on an individual basis. Does that make sense?

**M**
I think it's very clear, Neil. It's a very helpful observation. What we do with it, I'm not yet sure.

**M**
I guess the task and the scope here was to talk about what are the elements that increase trust in an exchange of health information.

**Neil Calman - Institute for Family Health - President & Cofounder**
Increase trust is to give true, informed, you know, true information about not about the good parts, but about the limitations of what we can do. I mean, because otherwise we go out talking about how we have all these mechanisms in place, and the newspapers report all the places that fails, but people don't really feel like we're actually informing them appropriately about what's taking place.

**M**
Yes, and so I think that would fall under this discussion section around transparency.

**Neil Calman - Institute for Family Health - President & Cofounder**
Yes. I think so too. I guess I'm suggesting that we need to put something in that's not just about the good parts, but also talks about the limitations.

**Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO**
This is Micky. Compliance will define what the responsibilities are of the stewards of the data, and then the transparency part, I think, Neil that you're getting at is the people, in this case consumers or patients, whose information it is, need to understand what the limits of those responsibilities are.

**M**
What I think Carol was talking about was transparency around the process.

**Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO**
Right. But Neil is getting at a different point, I think.

**M**
Yes.

**Neil Calman - Institute for Family Health - President & Cofounder**
Carol also said around the mechanisms, but also the findings.

**M**
Yes.

**Neil Calman - Institute for Family Health - President & Cofounder**
You know, so.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Right. I mean, you know, on the simplest exchange example, you could think about a certificate authority who issues certificates without proper levels of proofing and authentication or whatever. And that is observed … you want people to know that as soon as possible. In other words, the oversight is not a black box or a one time, once a year kind of check in.

**M**
And my thought is also the audit log function, both as viewed by a consumer, patient, and as monitored by an institution. We're not explicit in here in the concept of audit, not only in the sense of a snap audit by an outside party, but as routine mechanisms for audit, including the patient's own access. We've talked about another context, but we don't make it explicit here, and that makes me wonder if the word transparent is a little obscuring the way it's used here, and we should find some more transparent language that makes clear what we mean by oversight because we've talked in the last few minutes about three or four different variations of what we mean by it, and partly in terms of the process of transparency. Being able to say to the patient, here are the things we do to make sure this doesn't get messed up.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**M**
This is back to the e-patient Dave kind of scenarios. And you have a role, as a patient, to make sure it doesn't get messed up by looking at your results and so on online. That cycle of transparency and oversight is something that's not made clear in this discussion.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Yes, and a lot of that, I think, falls into, I mean, I always come back to FIP, to Fair Information Practice. A lot of that comes into the notice issues.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**M**
Right.

**Deven McGraw - Center for Democracy & Technology – Director**

Yes, it's both notice and, you know, to the extent that there is an ability to do more public education, in addition to notice, since so many people don't read them, even when we try very hard to make them understandable, obvious.

**M**
Leslie, could you move closer to the mic?

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Yes. I think we're not just talking about notice about practices. I think what Carol … more of reporting on what's happening, I think, pretty simply.

**M**
Right.

**Deven McGraw - Center for Democracy & Technology – Director**
It sounds like almost two levels of transparency.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Right.

**Deven McGraw - Center for Democracy & Technology – Director**
One is about transparency about what's happening, and the various protections that are being put into place in order to, while not insure because there are no guarantees, to do the best that we can to protect people's data. The other transparency is about transparency in oversight and accountability.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Correct.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
That's right.

**Deven McGraw - Center for Democracy & Technology – Director**
Maybe if we wanted to have a transparency slide that dealt with transparency about sort of functions, operations, what's happening, it makes sense for it to go here. There's also a transparency component to the accountability.

**M**
I wonder. Should we have a slide that's simply around transparency, and then have those two different sections?

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**M**
One is transparency of the process, and the other is – or transparency of the system.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**M**
The other is transparency of findings?

**Deven McGraw - Center for Democracy & Technology – Director**
Or transparency of oversight.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Yes, I think of oversight generally. That oversight is not necessarily a black box that people know what's happening and what's being found.

**M**
Okay. Let's move on to accountability, and then maybe we'll – or do you want to delve into, David, do you want to delve into the bullets?

**David Lansky – Pacific Business Group on Health – President & CEO**
Conceptually, my question is whether the bullet is right. Now the sub-bullets in particular on this slide is kind of a laundry list, a partial laundry list of mechanisms, and maybe we are realizing in this discussion that it both doesn't say enough, and it implies that we have a list of oversight activities, but obviously it's not an exclusive list.

**M**
Yes, I wondered. Would anyone objective to removing the sub-bullets?

**David Lansky – Pacific Business Group on Health – President & CEO**
I think we're going to reorganize it.

**Deven McGraw - Center for Democracy & Technology – Director**
I heard somebody humming.

**David Lansky – Pacific Business Group on Health – President & CEO**
Yes.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
…person….

**David Lansky – Pacific Business Group on Health – President & CEO**
I heard thinking going on.

**M**
None of that, none of that.

**David Lansky – Pacific Business Group on Health – President & CEO**
Any objections to removing the sub-bullets and recasting this in the way we just started discussing? All right. For the moment, we're going to go down the path of removing those bullets and recognizing this into two levels of oversight or transparency. But let's go ahead to the next slide and then come back.

**M**
Maybe the one thing on this section we do need to clarify is that oversight need not be governmental oversight.

**Deven McGraw - Center for Democracy & Technology – Director**
Need not be or isn't just about?

**David Lansky – Pacific Business Group on Health – President & CEO**
I think isn't just about. We've already said there's a lot of legal context for any of this. We know there's a governmental role.

**M**
Yes.

**W**
Okay.

**M**
I guess maybe we can be even stronger and say oversight must exist at multiple levels.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**David Lansky – Pacific Business Group on Health – President & CEO**
That's very good. I think that would get back to my concern about having a kind of cycle of oversight that includes institutions, professionals, the patients.

**M**
What Neil was talking about, that was organizational oversight that was involved there.

**David Lansky – Pacific Business Group on Health – President & CEO**
Right. There might be a very virtuous way to recast the slides and say that oversight is expected of all the parties, including the institutions, health professionals, patients, and external parties.

**M**
And there must be transparency at all levels.

**David Lansky – Pacific Business Group on Health – President & CEO**
Farzad, you wanted to look at the next slide…?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes.

**David Lansky – Pacific Business Group on Health – President & CEO**
Accountability and enforcement, number ten. I think Leslie and Deven began with raising some issues around how this is framed in terms of the strengths of the accountability, and I don't recall it now. Deven, I think you offered some language from the outset that would be a little firmer around accountability.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes, I'm trying to remember exactly what I said. Leslie, do you remember? Again, a lot of this is framed much more on the soft side, so you've got, and I think we agreed earlier in the call that there would be both language around accountability that is external, such as enforcement of rules by governmental entities and enforcement, for example, by other organizations, by contract, in addition to the exchange partners generally sort of accepting responsibility for what they're doing.

I'm almost wondering. I mean, I know we just got rid of some of those sub-bullets on the earlier slide, but they, to me, were a better and more clear list of the sort of various layers of enforcement and accountability that we're talking about here from government, through participation agreements, to individuals taking some responsibility for checking data, special obligations, etc.

**M**
Yes. And maybe it follows. Again, if we do rearrange these, to put the accountability up front and, again, not say they may answer to the other participants, individual subjects, government entities, or other third parties. Maybe here is where we, again, emphasize that maybe they must.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Yes.

**M**
Again, the multiple levels of accountability, multiple levels of transparency. But I think we have it here, Deven, right? Where we talk about, and I would put maybe the individual subjects first. Parties may answer to the individual subject, to the other participants, to other third parties and/or to government entities.

**Deven McGraw - Center for Democracy & Technology – Director**
Right, as long as the may is changed.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Right.

**M**
Yes. It could just say are accountable to.

**Deven McGraw - Center for Democracy & Technology – Director**
Right, or should be accountable to, must be accountable to.

**M**
The concept….

**Neil Calman - Institute for Family Health - President & Cofounder**
And we're saying that people are accountable to other participants. That assumes that some entity is going to take responsibility for developing those rules of accountability?

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Neil Calman - Institute for Family Health - President & Cofounder**
Correct?

**M**
The form that the accountability takes and the consequences may be different at the different levels.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
This is Jonah. I think one of the issues here is that who is actually policing this accountability? Is this all self-policing? Is there some – we mentioned other third parties, but we don't really describe who is ultimately … person in this role.

**M**
I think we wanted to establish the principle of accountability in the way we just started talking, which is right now essentially the second bullet and the first bullet brought together. Then we want to address the issue of policing and enforcement, but I think Neil is raising a third question, which is, what, from an NHIN point of view, which is our charter, who is going to lay out these accountability relationships and the mechanisms? It's fine to say, it could be this; it could be that. I'm sure contacts and circumstances vary. But from the NHIN point of view as opposed to the health information exchange more broadly point of view, we should characterize whether there is anybody in charge.

**M**
But you can have accountability without having – you can have a level of accountability to each other without having somebody in charge.

**W**
Right.

**Neil Calman - Institute for Family Health - President & Cofounder**
No, but you have to have some rules of engagement.

**M**
Right.

**W**
Right, but that's….

**Neil Calman - Institute for Family Health - President & Cofounder**
And somebody has got to do those rules of engagement.

**W**
Those can be by contracts.

**M**
Yes.

**W**
So there is kind of no reason that whoever is acting as the intermediary in the ID chain cannot be in a contractual relationship with all the parties who are exchanging, using them, for example, to exchange information, using them to authenticate.

**M**
I guess, Neil, what I'm saying is that what you're looking for will be there, particularly when it comes to the

formal top down government, you know, accredited organization, rules of the road, and so forth. But I think where we're going in this, modifying it in this conversation is to say, in addition to that top down, there are other important accountabilities that pertain to the partners themselves where you may say, you know what, I just don't trust those guys anymore. I'm not going to do it. I'm not going to exchange information with X hospital anymore. They've had too many breaches. Or a patient might say, you know what, I'm going to opt out of this, or I'm not going to go to that doctor anymore if they've had too many breaches. So some of it can actors acting on their own, as well as the clearly articulated, laid out, centralized accountability.

**M**
I think we need to go beyond the kind of good be theoretical framing that we have at this point. I'm thinking … Jonah and I working in the California context. You know, very practically, California is in the middle of laying out specific answers to many of these questions for California, and it's doing so in the absence of a strongly stated federal or national set of accountability mechanisms, other than the ones that are clearly stated from HIPAA and other federal requirements. But we could articulate at some point a hierarchy in effect that says, look, there's national law and a state law, and then there are going to be HIE requirements that are related to the NHIN contracting process, grant making process, etc.

Then there are going to be contractual relationships among parties, which are going to happen with or without us existing. That is, our committee has nothing really to say about that except we might want to offer guidance in some informal way. But HIE has been going on for while without the NHIN workgroup. In a sense, how are we as an HIT policy committee going to add value to this construct. And it may be by saying either the limits of federal guidance and, therefore, use the states, and private parties are free to do whatever you want that creates trust for you.

Or we should say no. We are going to provide a framework or some guidance or some regulation, which goes deeper into this category. But I'm worried about 50 states, and who knows how many localities having to answer all these questions themselves with a blank piece of paper.

**M**
I hear that, but let's remember that for these five is meant to be at the highest level of expression of what is required to have more trust in exchange, and I think it's not at the – we should keep this general enough that we're not being overly prescriptive for all different contexts of exchange, forms of exchange and so forth for these five bullets, these five slides, and I think we can have the implications of this framework for NHIN Direct or NHIN exchange in subsequent discussions.

**Neil Calman - Institute for Family Health - President & Cofounder**
I guess I'd just make one more pitch, and then I'll shut up, which is, I think when we're talking about RHIOs, it was clear that there was some government mechanism in all of this. Now we're talking about a different model of exchange, and I think it requires us to think through where the rules of that exchange are going to come from, and I understand that there's going to be all different types and all different everything, but just what are the rules? What's the framework within which this exists? And we struggle with this as a real live kind of a situation.

Who does need to be notified when there's a problem? What are the rules about passwords and other things? And I mean there needs to be some sense. Otherwise I think you sort of create the frame that everybody is sort of doing their own thing, and it's all kind of being done on a handshake and good will. And some oversight with laws, but the laws don't really tell you what to do in different circumstances. They just kind of create a very broad frame around everything. Anyway, I think we should go on. We

don't have to stop here, but it feels like there's a missing piece here for me, which is, who is creating the role.

**Deven McGraw - Center for Democracy & Technology – Director**
It's not one person, Neil.

**Neil Calman - Institute for Family Health - President & Cofounder**
Well, I know that, but where do they come from?

**M**
I would propose that for this, we say something like partners. It's a little bit stronger than "may". Partners must answer to or something maybe between … and us to subjects at multiple levels. Right, to subjects … to other partners and to a centralized entity, either direct government or through a third party, and that this may include penalties and so forth, but that the specifics of that, again, will depend on the context, the kind of exchange, and so forth.

**Neil Calman - Institute for Family Health - President & Cofounder**
Okay.

**M**
That we then delve into what those requirements are and what would be appropriate for the different context. Neil, I don't think you would want there to be, you know, a federal government rule that you would then have to follow for every time you want to do any sort of exchange, whether you want to fax something to someone or you want to call something with someone that you have to do whatever. Maybe you do. But the point is that it matters. It matters what kind of exchange that you're talking about.

**Neil Calman - Institute for Family Health - President & Cofounder**
Okay.

**David Lansky – Pacific Business Group on Health – President & CEO**
Let's come back to this slide as a whole, given this broad discussion. We started with thinking there's a need to strengthen the language about accountability, and I think we captured that. We have agreed that there are multiple levels of accountability and enforcement. We separated. We, in our conversation, separated three types of elements … bullet on here. After establishing the principle of accountability, we had the question of enforcement or policing in effect, and who sets the rules, which Neil raised. Any further discussion of how to capture that beyond Farzad's last comment that it will be done?

**Neil Calman - Institute for Family Health - President & Cofounder**
I guess the first, you know, there's a hierarchy here. The first thing is to be more, whether more explicit or just clearer about where these rules of engagement might emanate from or the various places they might, and then how that might lead to some upholding of commitments and enforcement. We start off by saying everybody is accepting responsibility for their own activities. Then we say we're going to uphold commitments, but I think we've got to start out by being more explicit about that.

**David Lansky – Pacific Business Group on Health – President & CEO**
Let me ask Mariann. In these last two slides, as the keeper of the discussion, if you feel like you've got enough to redraft these and circulate them.

**Mariann Yeager – NHIN – Policy and Governance Lead**

Yes, David. I think I got the gist of it, and I think we can pull something together and circulate it and get to, I think, what the group is aiming to achieve.

**David Lansky – Pacific Business Group on Health – President & CEO**
Anybody have any further comments on these two slides, numbers two and three, that they want to make sure we've captured before we see a redraft?

**M**
And do we want to flip the order?

**David Lansky – Pacific Business Group on Health – President & CEO**
I think that was generally important. Any reservations about that?

**M**
No.

**David Lansky – Pacific Business Group on Health – President & CEO**
All right. Let's move on then to the identity and authentication slide. I'm going to have to start moving toward another meeting, so I think Farzad kindly agreed to continue facilitating the conversation. I'll keep listening and chime in as I can.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Sure. This gets to, in order to have trust in exchange, you've got to know. You have to be confident that you exchange information with who you intend to exchange information with, that there has to be a validation and probably maintaining a record of the identity of those with whom information has exchanged. Again, to point out that the validation of the parties could occur in a number of ways. It could be recognizing someone's voice on the phone or someone's signature on a page up through using identity proofing and digital credentials to validate authorized members of a network.

The one point to ask your opinion about is whether we want to express this at the highest levels that pertains to exchange more generically, including some of the query and response types of exchange, or universal locator type of exchange, whether we need to have a sub-bullet here that relates to the identity of the subject of the exchange that confidence that you're exchanging information about the same person of the person you intend to. In those scenarios, it might be required as well.

**Deven McGraw - Center for Democracy & Technology – Director**
I think you're getting…. I think it makes sense, especially since this set of bullets is supposed to be overarching and kind of issue spotting at a top of trees level for a variety of different types of exchange, which might, in some cases, include query and response models. And certainly having, you know, a patient identification system or set of protocols in place is going to be important. Of course, it's a delicate issue because it kind of immediately – so often, unfortunately, boils down to the debate about the unique identifier versus thinking of it in a broader context. But on the other hand, it's like, if we don't mention it, we're arguably ignoring the elephant in the room.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
I kind of disagree with that. I would say this. I don't really think that you have to say that the issue of appropriately identifying the subject about whom you're exchanging information is important is a case that is unique to query and response. I think it is true, even in the simplest case. And I think, again, I always come back to FIP and sort of what that framework means.

There is an aspect, and I raised this, I don't know, on one of our past calls. There is an aspect of integrity of information and data quality that I know we've used in our framework that starts to speak to, it's not just the integrity of the individual that you're communicating about. But it's also the integrity of the information you're communicating with them. You have to be able to live up to those expectations. But I don't think it's an issue of, well, it applies to this kind of exchange and not another kind of exchange. It applies to the simplest of exchange.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. That's fair, Carol. I think I was thinking that in direct push models at least you were, you know, I was definitely assuming that the data holder would know whose data they were sending, but I can see that that's not necessarily always the case.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Not necessarily. I mean, even in a multispecialty practice or hospital, in the simple push model, patient's information may be in a number of databases. There may be one for patient registration and another for other pieces of information that need to come together. It doesn't necessarily only apply to the complex model. It is an issue, I think, good for all.

**Deven McGraw - Center for Democracy & Technology – Director**
But it sounds like it might be framed as a data integrity bullet.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I'd rather not create a new bullet, particularly since our focus is on transport, not content.

**Deven McGraw - Center for Democracy & Technology – Director**
Okay.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Yes. If the issue is just in the identity context, it's an issue of accuracy, the accuracy of the identity about the party, about the person about whom you're exchanging information. We could add something like that, but again, I don't think we're adding it because it only applies to complex data exchange.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Maybe to be more clear, the people exchanging information have to have some confident that it can be attributed to the person on the other end, to the person whom you intend it to be attributed to.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
That's right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right. Maybe we leave it at that because the reason to differentiate, Carol, between the universal locator, more complex searches versus the simple push, is that in the universal locator, that function is externalized to the network.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Yes, but that function still has to happen in some way.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**

It has to happen somewhere. I just don't want, if we put it too much as a requirement for trust that identity of the subjects be assured, then we have to be clear that that doesn't necessarily have to be done through the exchange mechanism. That could be, and in fact is typically done at the destination.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Right. It's actually not something you could outsource until you can do it yourself. If you can adjudicate identity inside of your own walls, you're not ready for a sort of outside, network-based, identity adjudication.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Do we have agreement then to talk about each has to be confident they're exchanging information with whom--

**Deven McGraw - Center for Democracy & Technology – Director**
And about whom.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
--and about whom. Thank you.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
--they intend to exchange information. I think that the last part of this, and that the other party is trustworthy probably again that encompasses everything here and probably has been dealt with in some of the other slides. The identity and authentication probably doesn't – what do people think about that last part?

**M**
I think it does start to blur the issues with what we identified in the second issue, or … enforceability. I think it blurs into that.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. I would take it out.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Otherwise this seems pretty good?

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Then we put last because technology should never come before policy.

**Deven McGraw - Center for Democracy & Technology – Director**
Way to go, Farzad.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I can learn. The technical requirements, and here we're saying that the partners have to adhere to technical standards that will allow for the secure, electronic exchange of health information, and that

clarifying that different kinds of exchange the technical standards pertain to different extents. So for a directed push, we are really focusing on, well, in some scenarios. I don't think this is actually quite right that the directed push follows the transport, but not content.

**Neil Calman - Institute for Family Health - President & Cofounder**
I don't think that's right either.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I think the issue is really, for example, may focus on transport, but not content, or transport plus other services, or the transport messaging and content.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Farzad, I want to raise, I think this should be redone for that reason, but I also want to emphasize that the technical standards are not just about secured transport and data content. The technical standards also fulfill or should be selected to fulfill the privacy and security requirements as well, the other ones, audit. You know, the other sort of elements of the privacy and security framework that need to be implemented through the technical standards.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I guess the question similarly, Carol, is how much of that are we ascribing to the network. Do we expect the network to fulfill the audit requirements, or will the disclosing entity do that?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
The nodes have to….

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right, right.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
…about that.

**Deven McGraw - Center for Democracy & Technology – Director**
Right, but not all of the elements of our trust framework are just applicable to the network. I mean, there's sort of a mix of network in edge system compliance throughout this whole document.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Sure. I mean, I think the first slide though where we started talking about that the participants in the exchange are going to hold up their end of their privacy and security requirements including, I would imagine, what the privacy and security workgroup is going to tell us around audit and so forth, audit and access and disclosures. So the rest of these, I'd like, I'm again concerned that we not have too much scope creep that may give a false sense of requirements to the exchange mechanisms, similar to the patient matching issue, Carol, that I don't want there to be a misunderstanding that we are requiring that for every form of exchange that there be audit built into the network, as opposed to … responsibilities of the participants. Does that make sense?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
I guess I was saying the opposite. I was saying there are requirements on the nodes, not on the network.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**

Okay. Requirements on the technical requirements that the participants must meet in the use and disclosure. I just don't want to get into the use piece.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
What do you mean the use piece?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Well, in terms of use and disclosure. Well, we're focusing on exchange, right?

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
What would partners have to adhere to technical standards to allow for secure electronic. I get your point. What would we add to this?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
It's the deficiencies in the example. So partners have to adhere to technical standards to allow for the – I would say the privacy and security requirements of the trust framework, and then I think the examples need to be fixed.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. You could say to support the privacy and security requirements of the trust framework. We often frame the technical pieces as being—

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
And I guess that's good because it then covers what you need to do for identity and authentication, as well as accountability, transparency, complying with law.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Right. Exactly. That's the point.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
But there's still a piece here around the technical requirements for the routing itself, which we haven't really talked about anywhere else.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Isn't that in the examples later because this is a trust framework generally?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right, but I think this also gets a little bit to the integrity issue that in order to trust in the exchange, you have to trust that exchange happens, not that it happens 90% of the time, but that the exchange actually took place without being altered in transit. I think that's maybe one of the sub-bullets that you're talking about.

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
This is Jonah. I think that's right. I think it's both the transport and the content and the structure of the content or the structure of the message. We have to consider that those receiving data believe in its integrity of the message that they receive. And if they do not trust that that message is, the content is what was intended by the sender, they can't trust the content, the package itself or the payload.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
The content is unaltered.

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes. And that the transport takes place.

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
Takes place, and in a secure way per the previous discussion.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Okay. Then this is an interesting point that Micky had raised with the administrative transactions back in the day that noncompliance with technical requirements may prevent an exchange from occurring, ideally will prevent an exchange from occurring, although noncompliance may not always be visible. So I think maybe the point this is getting at is, in an ideal situation, it is you not only – there's very good feedback on following technical, the technical specs, and that should be certainly visible, and in a way it is self-enforcing if it prevents exchange from taking place.

The one caveat to that, and I'd like to hear folks' views on is the concept of permitting what some term graceful degradation where, in this case, more if you were talking about the content, Jonah, where if there is noncompliance with the technical content standard, we may not necessarily want that transaction, may or may not want that transaction to automatically fair. You may want to allow the transport to occur at a lower level of semantic interoperability. So I don't know if the discussions around the second bullet are rich enough that it should not be dealt with so…. Can we express it clearly enough, or should we just delete it?

**Deven McGraw - Center for Democracy & Technology – Director**
This is Deven. I'm not sure what it means because, for certain technical requirements, we might not want to abide by, we might not want to allow noncompliance, but others, like if it's imperfectly sent, but it still gets there, that's not as big of a deal. I'm not sure what we were trying to talk about here.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
…means….

**Deven McGraw - Center for Democracy & Technology – Director**
Yes, well—

**Leslie Harris – Center for Democracy & Technology – President & CEO**
…you know, we assume it's being sent … secure protocols, so I'm not—

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
If it can't be sent securely with content unaltered, it shouldn't happen.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Yes. That's easier. That might.

**Deven McGraw - Center for Democracy & Technology – Director**
I guess I want to understand more what the exception was that we were trying to capture here.

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
Farzad, were you restating Micky's point? I just want to try to understand it that if some degradation of the payload may be acceptable?

**Leslie Harris – Center for Democracy & Technology – President & CEO**
That's what we're trying to figure out.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes. If we're only talking about secure transport, not content, then I think we could be pretty assertive in saying that if you can't insure that the technical requirements for maintaining the trust, including the identity and the accountability and that the transport actually takes place, acknowledgment, and that the content is unaltered. If that can't be provided, then the exchange must fail and fail completely. You know, the equivalent of, you don't want to get a garbled message. You know, if only eight out of the nine packets get through, you want the entire transaction to fail. On the other hand, if we're extending the technical requirements to the expectations around the content, particularly around the semantics of the content, then we may be less assertive about how that should trigger a failure in the transaction.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
I think we don't get it. We don't understand what that exception means.

**Deven McGraw - Center for Democracy & Technology – Director**
It sounds like we haven't defined it significantly precise enough, and it's at a level of detail that it maybe ought to come off of this slide and be put in a parking lot.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Micky, do you want to make a case for keeping it?

**Leslie Harris – Center for Democracy & Technology – President & CEO**
What is the exception? We don't get it.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
The exception is, Leslie, that if I send a C32 that is not perfectly well formed, that it got, you know, the person who I intended it, got it. It is the documents that I sent them. It hasn't been altered in transit, but one of the fields, instead of having this code set is using a different code set. Should that transaction fail?

**Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO**
Right. This is Micky. I think that's the question, Farzad. I mean, I like the idea of this, I forget what term you used, the graceful degradation or something like that. It does strike me that it's a real slippery slope.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Agreed.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. There might be circumstances where some graceful degradation of content is acceptable and others where it's not.

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
Right. I mean, I think we would need to define some logic whereby graceful degradation that doesn't result in a misinterpretation of clinical data that could result in an error of some kind is not acceptable, but some graceful degradation that is relatively—

**Deven McGraw - Center for Democracy & Technology – Director**
Harmless error.

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
Yes, harmless versus non-harmless error, and I don't know if we can do that.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
…I mean, it has sort of a meaning in law.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
It doesn't really have a meaning in technology.

**Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO**
Here's my proposal that we assertively state what we can assertively state.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Right….

**Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO**
And not be silent on the content degradation piece, which is much fuzzier.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes.

**Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO**

So noncompliance with technical requirements for secure transport.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Mariann Yeager – NHIN – Policy and Governance Lead**
This is Mariann. Just to be clear because since this is the overall trust framework, could you – I think at one point this may have read noncompliance technical requirements could prevent exchange from occurring.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I would rather be more assertive on what we can be assertive about.

**Mariann Yeager – NHIN – Policy and Governance Lead**
Okay. Very good.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Okay. That was great. We're now next moving into, or let me, before we move on, is there anything? Is this comprehensive? Do these five cover the ground?

**Deven McGraw - Center for Democracy & Technology – Director**
In a general way?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
At the….

**Deven McGraw - Center for Democracy & Technology – Director**
At the high level, I mean, especially since the one bucket of sort of business and legal and policy requirements is huge.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
That's why we gave it to the privacy and security workgroup.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Okay? So now we can—pretty much right on time—walk through how this overall trust framework can be applied to the directed push model. And to review, this is where the parties intend to send. The sender intends to send it to the recipient, and in the meaningful use stage one use cases that we used as our – have used up to now as our use cases for the directed push model, they are essentially all for treatment purposes or pursuant to the patient's right to their own health information.

With that in mind, I think, simplifying assumptions in place, let's see how the overall trust framework, what the implications of that are for what we need to have in place to have the trusted exchange of information in that scenario. So first, the agreed upon business policy and legal requirements, so again I think we're saying that it doesn't matter whether you send, I'm sending a piece of information to you by mailing you a CD or doing it using the secure routing over the Internet or by horse and buggy. That there's an expectation that is unchanged that once the information gets there, the privacy and security information will be protected.

We don't think that there are any disruptive privacy considerations of the directed push, and I believe the privacy and security workgroup on the consent piece in particular, when they looked at the simple push for treatment purposes. Deven, there was a discussion around this?

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. It's something that we are not going to officially report as done at the meeting next Wednesday. But so far, in part because we're thinking about when there's an intermediary in the middle versus direct push without the use of an intermediary. And we want to make sure that we're presenting this as a complete package, but essentially the workgroup is comfortable that there don't need to be any additional consent requirements than those that already exist in either federal or state law when you're talking about a direct push from the data holder to another, to the recipient, in part because that's sort of more consistent with patient expectations and is essentially digitizing the transport of information that either occurs today or should be occurring today.

So you don't have an issue where this day, you know, we're saying that this data can be shared with anybody and everybody in the world. In fact, we actually have some law about the rules for access, use, and disclosure of health information. They may not be as … down as some would hope. But, nevertheless, at least for stage one of meaningful use and all of the particular uses and disclosures in that category, people were comfortable that there wouldn't be additional consent requirements on top of that.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
And they point you raised about if there are intermediaries, what rules govern their use of the information, whether it's the metadata that is associated with the transaction or if in fact they're providing value added services, which require them, for example, if it's a transformation service where they actually have to open the package and the protections around consumer expectations around their reuse of that information either directly or the metadata associated with it is actually a specific case of a general issue around the reuse of health information, or secondary use of the health information by business associates and others.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
This is the key issue in identity online beyond healthcare. This is the question of whether or not we're going to have secure identities for transactions generally. It all gets down to this question, and other parts of the government are looking at this at the same point in time, and I'm just going to assume since some of that is not public that you guys know this because….

**Deven McGraw - Center for Democracy & Technology – Director**
You guys all talk to each other.

**Neil Calman - Institute for Family Health - President & Cofounder**
So for a simple guy like me, can somebody explain to me how this works? If I send a message to a specialist through some third party, and that message then is somehow captured centrally by the intermediary, are we saying that there's no special consent required for that, but if that intermediary then stores that information and makes it available through the exchange, then that requires a different type of consent?

**Deven McGraw - Center for Democracy & Technology – Director**

Neil, we haven't quite gotten that far. Essentially what we were comfortable with was the direct push from a data holder to another, to someone else. Let's say, in a simple transaction under stage one of meaningful use, this is you sending information to a specialist directly, not through an intermediary, but securely transported, you know, through however you're sending data now since you actually have an EHR.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
And the assumption there is an identity provider is bound by not being able to use or share because they're just providing … identity….

**Deven McGraw - Center for Democracy & Technology – Director**
Actually Leslie is jumping ahead.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Sorry.

**Deven McGraw - Center for Democracy & Technology – Director**
What we were able to get to in the privacy and security workgroup is direct exchange without an enabling organization in the middle, there is a comfort. But in your scenario, Neil, you identified an enabling organization that….

**Neil Calman - Institute for Family Health - President & Cofounder**
Exactly. That's what….

**Deven McGraw - Center for Democracy & Technology – Director**
They're not, and that's the issue that we're struggling with because how much access to data is there, so then you get to Leslie's point about when you're using an identity provider in the middle in order to either find the doctor that you're sending the data to or in order for your credentials, as Dr. Calman, to be presented to other doctors, so there's that trust that you know who you're sending to. She, on the other hand, knows that it's you who is sending to her. How much data does that identity provider collect? And, in some cases, so in other words, this is a struggle that's not just taking place in our healthcare conversations, but is a broader conversation that's happening about identity on the Internet generally.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
However, the identity provider ought to be, in most instances, a business affiliate and, therefore, is subject to rules, right?

**Neil Calman - Institute for Family Health - President & Cofounder**
Right.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
And we don't have any rules applying … in most of the other circumstances.

**Deven McGraw - Center for Democracy & Technology – Director**
Well, right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right. Two things: As Leslie said, in the health context, particularly, I understand, after ARRA, the business associates, and if an intermediary is a business associate, and maybe in this example probably would be a business associate who are bound in way that they are not if, for example, your Internet

provider wanted to use metadata about the Web sites you visit. They are, I understand, there's a brisk discussion about their ability to monitor, aggregate, and monetize that metadata about the information practices or whatever that you're doing.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
I'm just assuming that. I'm assuming they're business associates. Perhaps they're not.

**Deven McGraw - Center for Democracy & Technology – Director**
I think, in any case where they're performing a set of functions or activities with data that go beyond just merely for facilitating a transport, they probably are not. But it's a really open question.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I hope, Deven, that you're okay with me maybe paraphrasing or adding on that if the intermediaries are not merely providing routing without collection of persistence storage of information, whether it's direct data or metadata about the transaction for further reuse, then there may be additional privacy and security considerations around that.

**Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO**
Deven, I think you would say there will be.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
The question is may because if they're already covered.

**Deven McGraw - Center for Democracy & Technology – Director**
As business associates.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
As business associates.

**Deven McGraw - Center for Democracy & Technology – Director**
Right. We might not put anything additional on that.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
There may not be anything additional that is needed.

**Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO**
Yes, but I thought you were saying, Farzad, if you were to do additional stuff with it.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Well, even then, the question is whether you need additional protections, given that they are covered entities with rules about what they can and can't do, or what business associates of covered entities.

**Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO**
Yes.

**Deven McGraw - Center for Democracy & Technology – Director**

Right, although the business associate rules are the ones that are the least well understood. I think it's actually a little bit clearer of a question for some people about whether you'd put an additional consent requirement on top of that versus making very clear what they, as business associates, can do with whatever data they're holding, whether it's just data, PHI that's in the message envelope, or whether they actually have access to the payload. There's just an enormous.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
And there may be some policy principles that would be important to articulate.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Around, for example, maybe there shouldn't be PHI in the header.

**Deven McGraw - Center for Democracy & Technology – Director**
Right. Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Or secure transport, specifically if what matters is it goes from A to B. You need to know who A is. You need to know who B is, and you need to know…. But you don't necessarily need to know in the header whether that is accessible to the routing group….

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
I was going to say, I just hope we get to this level of detail because I think metadata in the header is a really dangerous issue, and if we could create a set of policies that say these are the right ways to do these things, and these are not, I think that would be very helpful to people.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Good. I will note again though that this is merely a special case, and maybe it's the point of the spear, but a special case of the much broader privacy and security policy issue.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right. Transparent oversight for the direct exchange, patients … exchange partners oversee and monitor to insure exchange occurs. Governmental oversight of compliance with laws, and oversight of third party that provides trust enabling functions, so this is the first time we are mentioning the need for a third party that provides any additional functions. I guess the question for the group to consider at this point is whether – well, let's do accountability enforcement, as we agreed before we jump into the transparent oversight part of it.

Exchange partners accountable to each other, to the patient, and governmental agencies, accountability may be extended to third parties that support trust enabling functions. That consequence for failing to uphold commitments to comply with the minimum requirements and code of conduct is termination of the exchange relationship between the parties. At least that's one consequence.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Right. Don't you think that needs to say one consequence?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
I mean … if they're contractual arrangements … damages.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes, and this gets to the accountability to each other part of it.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
But accountability to each other, I mean, it's possible. A household could decide to sue some other partner for failing to do something.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Absolutely, so this is neither complete nor either across the types of accountability, nor within the exchange partner accountability.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
I think it just needs to be written….

**Deven McGraw - Center for Democracy & Technology – Director**
One consequence.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
One consequence.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
A consequence or one consequence, so it doesn't sound like we're….

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right. So I guess the question to put on the table now is do we think, from a policy perspective, that to insure the adequate level of trust in the directed push of information that there needs to be necessarily government accountability, accountability to the government for these, for compliance?

**Leslie Harris – Center for Democracy & Technology – President & CEO**
There already is.

**Deven McGraw - Center for Democracy & Technology – Director**
There is to the extent that there are laws about what you can exchange data for. So that exists already.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes.

**Deven McGraw - Center for Democracy & Technology – Director**
So when you pose your question, Farzad, do you mean are they accountable to the government, for example, for meeting the technical requirements? Is that what you mean when you say no?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Or identity assurance.

**Deven McGraw - Center for Democracy & Technology – Director**
Or identity assurance, right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Earlier, I think, Carol, I think, paraphrased. I don't know if it's true. Correct me if I'm wrong, Carol, had maybe paraphrased … saying that the buck has to stop with the government to insure trust in a nationwide exchange.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Do we agree with that?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Absolutely. I mean, I guess I'm not sure of the context in which you're speaking now. Is this for health information exchange in general? I mean, I think just the fact that the trust framework and the privacy and security policies are being developed speaks to the role of government. But what is the context in which…?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
The context is directed push for this discussion, for the directed push of information to create a trusted, nationwide mechanism whereby, for example, any provider could push information to any other provider, and we would meet the elements of the trust framework, including the identity assurance that you know there's confidence that it is who the person says they are, and they get it, and that the package isn't altered, and there's compliance with the technical standards and so forth. Is there a need for a government enforcement mechanism for the directed push above and beyond what's already in law?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Yes. I would say the different elements of the framework merit different elements of enforcement, so if the government is going to establish entities that are appropriate or authorized to issue certificates, for instance, then there's a certain oversight and enforcement mechanism that's going to come with that. The issue of data, you know, enforcing data integrity is different.

The issue of two parties creating mutually agreeable policies for what they're sharing and how they're going to enforce that, whether that means if someone on one end of that contract is fired because of inappropriate use of the information or whatnot, those are other levels of enforcement. I think it's important that the overall framework get established and the, you know, for me it's hard to do this divorce from the privacy and security framework, so Deven may be closer to that or know how they're looking at the enforcement element because these are all part of a piece, and they do need to get looked at as a package.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
You know, one of the asks or part of the charter of this group, though, is to make recommendations about whether and how a governance framework may be required, and that there's, I think, very specifically a

question of whether a regulatory framework needs to be established by the government to govern the nationwide health information network. I think that's where we really need to, first of all, be able to say, do we think there's a need for any government regulation above and beyond what's already in place in order to insure trust in a nationwide system for directed push of information to satisfy stage one meaningful use requirements, for example.

**Deven McGraw - Center for Democracy & Technology – Director**
And we're assuming, when you use the term directed push, there's no intermediary, including there's no identity. There's no certificate authority in the middle. Do we think that's even going to likely be possible?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
No. I think actually that that may be part of what gets – an important part of what gets regulated are enabling organizations because, if we think about 100,000 small offices, office practices, and the requirements for not only on the technical side, but also on the identity assurance side, in order for this to really scale nationwide, at least in some instances we have to be able to account for the participation of enabling organizations other than the provider organization themselves.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
The question is whether there needs to be regulation of those entities.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. And as we've already discussed, we think that the government, through the business associate provisions, has authorization to regulate them, but I don't think, at least in my opinion, they're not as regulated as they need to be or as clearly as they need to be in these contexts. So on the one hand, does the government need any more authority? One could argue no because they have it. But that authority is maybe imperfectly implied at this point, so it's not the case that we don't need additional rules, that the government would be responsible for enforcing. It's a slightly more nuance expression of your point. We don't need new government, but we need government to act in more specific ways than is the case today, I would say.

**Adam Green – Progressive Chain Campaign Committee – Cofounder**
This is Adam Green with the Office for Civil Rights. A couple of points that I wanted to add to that, there's a proposed rule in the works that's going to add some more specificity to the obligations and compliance requirements of business associate.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Yes. Sorry.

**Deven McGraw - Center for Democracy & Technology – Director**
Sorry. Thanks, Adam.

**Adam Green – Progressive Chain Campaign Committee – Cofounder**
And that's going to be – I can tell you that the proposed rule went to OMB earlier this week. That's on the OMB Web site. That's as much as I can say about the timeframe. But it will be a proposed rule. It's not

going to be a final rule, so there'll be opportunity for comments on what more needs to be done potentially in the area of business associates.

Another thing, though, I would like to point out is government really enforces kind of the minimum, so HIPAA, for example, was the floor. And the expectation is there's going to be potential best practices higher than what the government mandates. And so that's one thing to keep in mind. And part of that is also regulation. The regulatory process, as people are seeing currently, is not something that turns on a dime. It takes time, and as the technology develops, it could be difficult to maintain kind of best practices for trust through strictly a regulatory framework.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Adam Green – Progressive Chain Campaign Committee – Cofounder**
Looking to government to enforce best practices can sometimes be challenging rather than looking for government to enforce kind of a bare minimum of you have to meet these minimum requirements.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Okay.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Well, but that is why there's going to have to be.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I think that, again, thinking about the frame that we're talking about, there's a base.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
That base may be becoming more detailed, and then the question is, on top of that base, what additionally is required to enable specifically secure routing in the directed push.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
And if we're talking about, for example, the certificates, it's possible that the proposed rule will talk about a nationwide route certificate authority for business associates, but it may not. So maybe we can talk generically about what the needs for government regulations are for this particular application of business associates, and we can then, once the rule is public, we can then talk about how much, above and beyond what's already in the proposed rule, would be required to insure trust in the health information exchange. Does that make sense?

**Deven McGraw - Center for Democracy & Technology – Director**
I think it does, but I think the bottom line is that it's not going to, at least I don't think we would feel comfortable saying that there's no more government authority needed until we sort of think more about what specifically we want to see in this space, what's already covered by rule, and what might need to be added, and what's the best way of making that happen.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
That's exactly what I'm suggesting, but I guess I'm saying let's draw the line of what we think there needs to be government regulation of, and then we can look to see how much it's going to be covered, is currently covered, and may be covered in the future, and what is the space. ARRA specifically asks the Office of the National Coordinator to look at governance of the NHIN.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
So I think we need to look at that. So let's start with the government, the portion of this that we think is essential to have some governmental role in, and define that as well as we can, and then move on to what might be in the directed push example, the accountability to exchange partners, as well as patients and see how that might be worked in here in a little bit greater detail. For government regulation or government accountability and enforcement, if there are enabling organizations, then the sense was that there does need to be federal regulation. Do we want to say federal, or could it be left to the states?

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
I think we need to leave some latitude to states who have different rules.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Jonah, does there need to be federal regulation and, of course, states go by HIPAA, right? States can go above that and do their own.

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
But does there need to be a base of federal regulation?

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
Yes. I think there does and there is. Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Then there'd need some federal regulation of those enabling organizations, and specifically relating to what?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Farzad, I'm kind of lost on this because I don't know that I understand what the enabling organization does. Every time you mention it, I understand an enabling function, like providing an authorized certificate, a valid certificate or what have you. But I really have a problem when we start talking about organizations because it makes it sound like these elements get outsourced to some third party. Then the government sanctions third parties, and I'm not sure that's true. I think a lot of the elements of trust framework have to get implemented by the nodes, and that the oversight and accountability and enforcement of those policies have to be thought of as part of a whole, and therefore, I'm not understanding where you're driving.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**

That's a good point. The presumption, I guess, is that let's talk about the functions, so identity and authentication. There may be someone needs to vouch for the identity of the provider, the node, as it were, in your example, right, Carol?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Sorry. I'm not following.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
You're talking about the functions needed for trust, for identity assurance and authentication. Somebody has to vouch for the identity of the node, yes?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Correct.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
So does there need to be government oversight and regulation over the groups that are recognized as being able to vouch for the node?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
I would say yes because the first time someone vouches for a node and does it inappropriately is the beginning of a lapse in any kind of trust.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Okay.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
All right. That's good, so that's one function. The other is around the technical specifications for the routing itself. So the statement that we've heard is that it is not the small doctor's office who wants to participate in exchange from one group to another. They may lack, in fact, I know that they lack the technical wherewithal to do that or the interest, frankly, in doing that, maintaining that certificate, formatting the message and doing the routing and addressing and maintaining their address on a directory directly. So they very well, we need to plan for a world where they would contract with other organizations to provide them with that functionality.

That may be their electronic health record vendor. It may be their professional society. We've seen examples where it may be a hospital. It may be others who would provide that practitioner or that node with the technical capabilities around the maintenance of the technical, the certificates, the encryption, the routing, the addressing, the directory and so forth. So there need to be government oversight over those enabling organizations.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. I think so. This is Deven.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right, and particularly in the context that in routing, performing the routing.

**Deven McGraw - Center for Democracy & Technology – Director**

Yes. There's where I'm sort of more hopeful that it'll be clear that those folks would be business associates.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes, and we could plug into existing regulation around those business associates.

**Neil Calman - Institute for Family Health - President & Cofounder**
But if they were vendors, would that become part of the certification process for vendor products?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Let's hold for a moment the method of government regulation of them, and I think it might or might not be. We have to consider a general enough case that it covers a variety of potentially enabling organizations, not just vendors though.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
I just want to say one more time, I really think it's a mistake to talk about enabling organizations for every….

**M**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
For what?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
I think it's a mistake to talk about enabling organizations for every one of these functions. These functions may not be lumped together, and they may not be performed…. I think it's much better to talk about the functions that are part of the trust framework that may be performed by organizations instead of trust enabling organizations, which implies some homogenous set of things that third parties uniformly provide.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Fair point. One reason, Carol, to make it concrete, to talk about organizations rather than functions is that regulation occurs over legal entities.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Right. I understand that, but regulation can occur over legal entities performing functions that are required and should be over functions that are required as opposed to implying that there is a single kind of organization that performs all of these functions as a package. They may not all happen in one entity.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Sure. So maybe we can talk about identity assurance enabling organizations or vouching organizations and routing organizations, enabling organizations rather than a unitary rubric of trust enabling organizations that, as you say, may imply that – and it may turn out that way, but it may turn out not that way. I take your point.

Okay. So for the minimal, the identity and authentication, and the minimum technical requirements, we've said that there does appear to be a need for organizations to act at times on behalf of practitioners, and that those organizations do need to have some government, federal at a minimum, regulation and

oversight and accountability. And I think that's good to be able to at least move forward to that extent. Any other thoughts on this? I would like to get to the – go ahead.

**Neil Calman - Institute for Family Health - President & Cofounder**
I guess I'm just going back to Carol's point because the way I'm seeing this in my mind is that it is going to be disintegrated, and isn't it that we're sort of giving people, we're saying that there needs to be a license to do the function. There needs to be a license to do the identity piece, right? There needs to be. I guess I'm just trying to think through, so what's the next implication of this? How does that actually get actualized? If you doing different things with different types of organizations, are there rules that they have to comply with? Are there requirements being put on the entity or on the process that the entity is doing, and how is that going to happen? I know you don't want to get into this level of detail now, but I think to do something at a very high level, but not be able to sort of describe how that might actually take place doesn't leave me in a very good place.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Arien, are you on the phone? Arien, you may be on mute if you're on. Okay. I was hoping that Arien could speak more concretely about some of the models.

**Neil Calman - Institute for Family Health - President & Cofounder**
We can leave this for a future discussion if you want.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes. I do think that we're going to get there.

**Neil Calman - Institute for Family Health - President & Cofounder**
Okay.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
But I'm sensitive to not jumping to a particular model. We did that as part of one of the policy committee discussions, and I think it was not as clarifying as we had imagined it would be.

**Neil Calman - Institute for Family Health - President & Cofounder**
Okay.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
But moving on to the other pieces that I think was a really important observation in today's call that accountability enforcement is not purely a federal function or a government function, that exchange partners need to also be accountable to each other. How could we see that other than, and maybe it's only the consequence, as it's saying here, that a consequence for failing to uphold commitments would be termination of the exchange relationships where basically you get on my something list, and I say, I'm not going to exchange information with that person again. Leslie mentioned that there may be other contractual violations that could be built in. Does someone want to follow that thread?

**Neil Calman - Institute for Family Health - President & Cofounder**
That's not normally the way we do things when we're trying to improve processes and make things work in the future.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
I agree, and I was actually thinking less contractually about the two ends of the exchange and more about the middle.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I don't think, Leslie, we're talking about a middle, middle.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
I agree we're not talking about a middle, middle. I think we're, at a minimum, talking about identity providers, so questions of trust with identity providers can be you don't use them anymore. It can also be that there are some consequences for their failing to do what they're supposed to be doing.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right. As long as there's transparency, and as long as they're providing a market good, then there would be potentially severe implications for them as businesses for failing.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Right. That wasn't really addressing the contract to the end.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes. I would propose that we may want to take it a step further in that if one of the parties fails to act in accordance with the rules and law that they just don't get – it's not just about that exchange between those two entities being terminated, but that that entity that fails to meet the rules cannot exchange information with others at all until the situation is rectified in some way.

**Neil Calman - Institute for Family Health - President & Cofounder**
I think we're at an early stage in the process, and I can tell you from firsthand experience that when you start down this path, there's all kinds of things that go wrong. What you want to do is use more of a quality improvement model here, I would think, the same way you do in other aspects of critically important healthcare. You don't want to say to the thousands of patients that use a facility, sorry, this facility messed up once and, therefore, your information is no longer accessible to others and they no longer have access to any of your information. That doesn't really benefit the users of that doctor's office of facility.

I think we need to think this through more in terms of more of an improvement model that there needs to be a plan of correct, that there needs to be some sort of documentation of the incident. There needs to be some approval for the plan. That's why I'm trying to think who's doing this kind of stuff. But I think the sanction mechanism early on isn't exactly where you want to get.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes.

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
I do agree that you do need to have a quality improvement mechanism, but if an institution violates a rule, and if it happens to be that they're selling their data to a third party, I do not think it is in the best interest of any patient that that institution is allowed to continue to trade until they remedy.

**Neil Calman - Institute for Family Health - President & Cofounder**
Right, but I think we think about different examples, so that's the example you're thinking about, and I'm thinking about an example where information gets pushed into a provider, and the information is left all over the place and is not appropriately secured, and somebody gets their hands on it, and there's a breach for a particular patient in a particular circumstance. Where somebody needs to then correct a

procedure or people are sharing passwords, so somebody who shouldn't have access to that information gets it. The provider needs to do a better job at securing passwords and access to the exchange.

There are all kinds of things like that that aren't, you know, gross legal, criminal violations. Those are the things that I'm thinking of because those, I think, are going to happen 100 times for every one time somebody goes out an intentionally sells the information.

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
Again, since this is a trust framework, I think the examples you brought up are consistent with if a provider is, for example, negligent about how their information is locked down, and there are breaches, or they're sharing passwords inappropriately. Then it would be very challenging to maintain a trust framework if that provider has continued to be allowed to exchange and receive information when they're in violation of some basic rules. So they should be allowed to remedy. There should be a corrective action plan, but we should not continue to allow them to exchange feely with others until they've met the minimum requirements.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Was that Jonah?

**Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I guess the question is whether that is a centralized set of process and set of rules, or whether what's established is transparency and the decisions about that are left more to the individual exchange partners.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes. I'm sitting here listening to these examples and thinking these are some areas where we actually have law.

**M**
Right.

**Deven McGraw - Center for Democracy & Technology – Director**
And some accountability, and so if in fact you've got an organization that has a data breach, they've now got reporting obligations, and the government authorities may or may not impose additional sanctions. But what does that mean for exchange, and do we count on – so if we cut those people off from exchange, who does that hurt?

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Right.

**Neil Calman - Institute for Family Health - President & Cofounder**
Exactly.

**Deven McGraw - Center for Democracy & Technology – Director**
I'm a little reluctant. As much as I'm a fan of enforcement, I sort of – you know, there's a point at which there's got to be some individual responsibility on the provider to make some – they're going to make some decisions about who they exchange with, and this notion of trust, there's a strong role for the

government to play. But it's not – and for participation agreements to play. But, at the end of the day, especially in a push model where you're deciding who you're exchanging data with, you've got some decisions to make.

I guess, Jonah, I got a little uncomfortable. They can't exchange data anymore. Well, what about the patients of that provider?

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Right.

**Neil Calman - Institute for Family Health - President & Cofounder**
Right. That's why I'm saying, in healthcare, in medical care, there are processes for dealing with things like this. What you try to do is use these to inform improvements, not to sanction people unless there are repeated violations and stuff or unless there's criminal activity, criminal negligence, something like that. But otherwise, you use problems to inform improvements so that you can perfect the system. And if you keep basically taking people early on in this process and sanctioning them, there's going to be nobody left because nobody is going to enter into this space without having either individual or other kinds of problems with security.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
The other point that's been made is that if a sanction is too heavy, then the likelihood that it gets imposed ever falls exponentially.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Right.

**Neil Calman - Institute for Family Health - President & Cofounder**
And also that people realize if providers realize they can't control every aspect of it, but yet they're subject to sanctions that are out of their control, they just won't play.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
I think we're making the same mistake again, which is to talk about all violations in one breath and, therefore, all sanctions.

**Neil Calman - Institute for Family Health - President & Cofounder**
Yes.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
We really have to do this in the context of policy framework. I know I sound like a broken record here, but each one of these policies and violations of those policies comes with different opportunities for enforcement and sanctioning. For example, one of the most common misuses today or breaches versus a breach today is an authorized entity with an authorized user end up looking at something they're not supposed to look at.

You know these cases of somebody looks up someone in the hospital that they're not supposed to look up, a celebrity, what have you. The way those are commonly dealt with is not to say this entity is now prohibited. Most contracts today between entities that are sharing information have the provision that says if someone on your end uses the information that I'm sending you inappropriately or looks up information inappropriately, you'll take measures to terminate them. That's typically, you know, termination is typically handled for the individual behavior in a situation like that.

But again, I think we're lumping a lot of different potential violations in one bucket. There may be situations where the violation is egregious and, therefore, it is appropriate to say, you know, this entity has to make – has remediation to do or what have you, but I don't think we can take it all as a homogenous violation. There are lots of different aspects to this based on the individual policies.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
In deconstructing this big bucket, it appears to me that there is a whole series of things, and most of what these examples that I've heard so far have to do with the use of information within the organization, use or misuse, and disclosure or inappropriate disclosure or breach of the information once it has been exchanged.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I'm not sure if the instrument to deal with those is through all these different exchange agreements so that the sanction for that is, well, I'm not going to share my information with you because you have a lot of breaches. While it appears, again, the work of the privacy and security workgroup should talk about that someone has an HR policy that they terminate someone who looks inappropriately or if there's a pattern or whatever. But that shouldn't be in exchange agreements. That should be a general policy that is promulgated.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Right.

**Neil Calman - Institute for Family Health - President & Cofounder**
But if there are two organizations exchanging, and one organization's HR policy is that somebody gets suspended for a half a day for their first offense, and another one is that people are immediately terminated, there's got to be something about how these things are handled, some sort of process.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes. I guess what I'm suggesting again is for us to be careful of the roles of the NHIN workgroup and the privacy and security workgroup. I'm really glad we have Deven and others who can speak on both sides. But for our scope here, I think it would be – the piece that really we have to address is the exchange related, the things that are directly related to exchange.

**Neil Calman - Institute for Family Health - President & Cofounder**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Focus on, at least initially, the misuses or violations, as they pertain to the exchange of information itself. So if the identity assurance provider doesn't do a good job, there's clearly we've talked about the need for federal regulation about it. There may be state regulation over that, but are there implications in terms of the people that contract with them to provide those identity assurance services. I would imagine there could be. If there's a routing enabling organization who loses packets in the mail, there should be consequences for that from the business side, as well as through government regulation, as long as there's transparency around that.

**Deven McGraw - Center for Democracy & Technology – Director**

Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I think the key here is that the government regulations should provide for transparency that would enable these other mechanisms to operate. Does that make sense?

**Deven McGraw - Center for Democracy & Technology – Director**
I think it does, Farzad, in part because the way that you framed it is both a combination of regulation, as well as market forces of which transparency is a key component of that, and especially under a direct push environment where providers are, you know, if we do this right, and if we're lucky, there'll be multiple services that a provider may choose to use in order to do identity proofing, for example, or to do secure routing if they feel like they need. And, in which case, if you have a lax provider out there, you've got both, you know, the failure to abide by baseline rules from a government standpoint, but also why would you exchange data with somebody who is lax with, who doesn't handle those functions responsibly.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right. As long as we deal with the information asymmetry market failure.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
How about patients? We talk about patients, you know, the exchange partners being and the sources of data being accountable to the patient. How can we make that? Is that in place today?

**Deven McGraw - Center for Democracy & Technology – Director**
Are you talking about patient accountability in the context of provider-to-provider exchange, as well as provider-to-patient exchange?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes.

**Deven McGraw - Center for Democracy & Technology – Director**
You know, that's, I think, in part what the role of government is. Again, that's why you need the baseline rules, and you can't necessarily just count on the market because the patients don't make the choice about what identity provider-to-provider uses.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
But if the provider screws up, is there, other than the government acting on behalf of the public interest, right, in the public interest, on behalf of the patient, is there a way to – does it exist today? And if not, is there a way to enable patients to more directly hold their providers and their business partners accountable?

**Neil Calman - Institute for Family Health - President & Cofounder**
I think there's a step before if the provider screws up, which is, if the patient finds out about the provider screwing up or how they know if the provider screwed up.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes.

**Neil Calman - Institute for Family Health - President & Cofounder**
And to what extent do they have access, direct access to things like the audit trails on their records and the ability to be able to get information that's intelligible about whether their privacy has been breached. I mean, it's a very complex problem. I think the easier part is what happens once you know. I think the harder part is how do patients find out.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Adam?

**Deven McGraw - Center for Democracy & Technology – Director**
Yes, it's Adam. I mean, you know, we now have mechanisms for that that we didn't necessarily have before. One is the breach notification requirements for those things that qualify as breaches.

**Neil Calman - Institute for Family Health - President & Cofounder**
Right, which is not everything.

**Deven McGraw - Center for Democracy & Technology – Director**
It's not everything, but then there's also the new accounting of disclosures rule where providers with electronic health records are, upon patient request, are going to need to tell patients about disclosures from their record. This applies not at, I mean, this applies at the node level, and we still, you know, there'll be some regulations to implement the technical standard that was in the certification IFR, and it only applies when electronic health records are used. There are a lot of unanswered questions, but we at least have some vehicles on the table from a sort of government … you know, going back to the government compliance piece of this that we didn't have before.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Now is there a role for – do the patients only have a role in accountability of the providers, the medical providers, or do we think it might be appropriate in any way around the routing enabling organizations, for example? I see that as being much more of a tenuous connection.

**Deven McGraw - Center for Democracy & Technology – Director**
Do you mean are the routing organizations accountable to patients in some way?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes.

**Deven McGraw - Center for Democracy & Technology – Director**
Well, again, to the extent that we've got government regulation on the table for them, then the government, through its public accountability function, is supposed to be acting on behalf of the patient.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
But if a routing organization, I guess I don't know if there's clarity in the regulations around this. Folks, just let me know.

**Deven McGraw - Center for Democracy & Technology – Director**
We'll know when we see them.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I guess what I'm saying is around the – okay. It's a fair point.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes. So if a business associate does a breach, whether there might be – well, let's talk about what we think would be a good thing in this context. Would there be a primary responsibility of the business associate or, in this case, the routing organization for direct, say, notification of the patient?

**Deven McGraw - Center for Democracy & Technology – Director**
No. And, in fact, the law is very clear that it's not. To the extent that the routing organization is a business associate, their obligation is to notify the provider.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
The provider.

**Deven McGraw - Center for Democracy & Technology – Director**
The provider, who then notifies the patient, so in some ways the accountability runs. The accountability of patients is both a governmental function, and then one could argue providers acting on behalf of their patients because essentially when they exchange data, they're doing so for patient care purposes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
One special case of that is where we are enabling provider communication to a patient designated entity.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Right.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
And those may not be business associates of the provider.

**Deven McGraw - Center for Democracy & Technology – Director**
Right.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Right.

**Deven McGraw - Center for Democracy & Technology – Director**
That's right.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
That's right.

**Neil Calman - Institute for Family Health - President & Cofounder**
They're likely not.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
I think we have to say they may not be.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Do we need to – does this workgroup need to address the issues of the accountability and transparency and enforcement for those patient designated entities who would receive the patient's information on behalf of the patient, or is that also covered by the privacy and security workgroup in their looking at the non-covered entities, for example?

**Deven McGraw - Center for Democracy & Technology – Director**
We're going to look at what should be the privacy and security policies that apply to those entities when they receive the data. But to the extent that there ought to be some requirements on the data transport piece from a provider to those entities, particularly when they're not covered by HIPAA, but even when they're not. I mean, ideally there ought to be some consistent rules where we're dealing in an environment of a bit of uncertainty here because, in some cases, those entities will be regulated as business associates, and sometimes they're not. But the ideal is that there's a consistent set of rules.

One could argue that insuring the data download piece is part of what this workgroup could have some responsibility for, but the rules about what that entity can and can't do with data is something that the privacy and security workgroup ought to focus on. Just in the same way that you sort of drawn a line between the exchange piece that this workgroup would handle and what the nodes are responsible for complying with from a privacy and security standpoint.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Would you also be looking at the identity assurance requirements for patient designated entities?

**Deven McGraw - Center for Democracy & Technology – Director**
That's a good question because we haven't, in terms of a work plan that's coming down the road for us, but to the extent that that's something that needs to be decided very soon in order to facilitate stage one of meaningful use since those pieces are in there. I don't think it would hurt to have this group tackle that. But we don't have to necessarily decide that on this call. It's an extraordinarily important issue that I don't think it's squarely in one bucket or the other.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
David Lansky, the guy has foresight. Three months ago, he talked about whether we're going to need to wade into those waters or not, and we kicked the can down the road. And I think, here we are at the road.

**Deven McGraw - Center for Democracy & Technology – Director**
Then there are all sorts of ways, as we know, that patients are going to want to receive data from their provider. Some of them, for example, will use PHRs, but some won't. Some will just want a simple way to get an electronic copy that they might store on their own hard drive.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
We're into rulemaking, Deven.

**Deven McGraw - Center for Democracy & Technology – Director**
Right, I know, but you don't have to say anything. I'm not asking it as a question, but I'm throwing out there that….

**Leslie Harris – Center for Democracy & Technology – President & CEO**
A lot of people are just going to … you know, stuff delivered to their e-mail using their ISP and all of the traditional Internet exchange protocols, and they're going to get it, or they're not going to get it.

**Deven McGraw - Center for Democracy & Technology – Director**
Right. Carol can jump in on the work that Markle is doing on sort of facilitating an easy process for patients to get data, whether they're using some PHR or consumer access service or not. Maybe we lost Carol. At any rate, I understand that there's sort of a pending rulemaking, so you don't want to be too specific here. To the extent that there are some policy guidance that's needed in that regard, we can talk about what's the most expeditious way to get that on the table and get it done.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Just to summarize—

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
I'm here, by the way. I was on mute. Sorry.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Carol, do you want to say something about the work Markle is doing around the consumer, the responsibilities of patient designated entities for their use and reuse of information they receive on behalf of the patients?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
What I would say is we developed a framework for that very use case more than two years ago on sort of network personal health information that goes through every one of the policies and practices of fair information principles and got pretty detailed about some of these issues, so I'm happy to provide that as a reference. In the context of—

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Is there a rule for – I remember that there was broad acceptance of that by some of the leading—

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
Yes, 55 organizations in fact.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes, so was there anywhere in there a need for government regulation?

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
At the time that we did that framework, that possibility wasn't on the table. But we did identify, as Deven knows, in the enforcement section some opportunities for both oversight and enforcement at the government level.

**Deven McGraw - Center for Democracy & Technology – Director**
That's right, and CDT has actually used that, the common framework for network personal health information to develop the paper, which we're releasing soon that does call for a government role to enforce some of the baseline recommendations that were in the common framework.

**Carol Diamond – Markle Foundation – Managing Director Healthcare Program**
The other issue I would point out, which we relied on when we developed the framework as well is to the

extent that entities post policies on the Internet, that they're accessible to consumers. The enforcement of those policies and the handling of breaches in those policies does also trigger FTC involvement.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
In terms of these slides that we hope to be able to present after editing and turning it around for you folks, I think we want to call out the potential need for policies. Let's just go through, agreed upon business policy and legal requirements. I think we want to call out the potential additional policies required for routing enabling organizations use of, if they are to use either the metadata or the content. You know, open up the package as kind of the exhaust gas of performing the transport.

We want to talk about, in the second bullet around transparent oversight, that maybe putting in first government oversight of compliance, but also government regulation of identity assurance organizations and routing organizations, but also that part of that regulation should enable transparency that would facilitate patient and exchange partners to perform their – this is where the transparency comes in – to be able to enforce and hold accountable the exchange partners and the identity assurance and routing organizations.

An open question to me whether we put in here specifically the patient designated entities as something for us to consider either on the identity assurance side or on the government regulation side. Maybe we just say must be dealt with, and without specifying who is going to deal with it. Is that okay?

**Deven McGraw - Center for Democracy & Technology – Director**
I guess I'm getting confused because I'm looking at the slides, and they're saying, legal agreements, but I assume – is that the context in which you're raising this, Farzad, or something different?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I'm going back to slide 14 and talking about how we're going to alter these bullets to reflect the conversation we just had. So on the first bullet, other policies, and I would then specify other policies and then specifically relating to the use by other organizations of the metadata or data, right, as a byproduct of the secure routing needs to be addressed.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Under accountability and enforcement, I think we want to say that this group thinks that there is a role for federal regulations around if there are enabling organizations around identity assurance or routing, that that regulation must include the creation of greater transparency that would enable patients and exchange partners to hold accountable the regulated entities.

Moving on to slide 15, whether – I think here we want to add in another sub-bullet around the issue of identity assurance for patients must be considered when it comes to patient designated entities for receipt of their … access to patient information. And I think minimum technical requirements are pretty non-, we didn't really talk too much about it, but I don't see – I don't know if folks want to comment on these.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
The minimum technical requirements, we're not including patients here, right, or are we?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
We don't have.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Well, I see PHR….

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
PHR, yes.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
I do see the word PHR.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Well, but it's in the context of EHR-to-EHR, which I don't think is really there.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Right.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I think we should add the EHR to PHR as a separate. Well, we'll talk with Arien and the NHIN Direct group to see if this is something that they're considering in their technical requirements. I believe that is one of the later use cases that they're going to consider.

**Leslie Harris – Center for Democracy & Technology – President & CEO**
Okay.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Okay. Moving on to slide 16, I'm not sure if this belongs as a separate slide or not.

**Mariann Yeager – NHIN – Policy and Governance Lead**
It was one of the elements and one way in which the trust … could be implemented. In another group, it talked about at one point or another—this is Mariann, by the way, sorry—it could be implemented through some form of legal agreement. So it was just there was a placeholder to see if … that fits.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Right. If we've developed the framework with the five, and then we apply it, we shouldn't add a sixth, it seems, unless this is—

**Mariann Yeager – NHIN – Policy and Governance Lead**
This would be one mechanism….

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
One mechanism in addition to government regulations.

**Mariann Yeager – NHIN – Policy and Governance Lead**
Right, in addition, so it could be woven in if, for instance….

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**

Yes, I would weave it into the accountability and enforcement and the business policy and legal requirements sections. Okay. This is a public call. We should hear from….

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Yes. Okay. Operator, can you check and see if anybody on the line from the public wishes to make a comment?

**Operator**
We do not have any public comments.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Thank you. Farzad?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Thank you. Any other last thoughts from the workgroup members?

**Deven McGraw - Center for Democracy & Technology – Director**
I just want to understand the process a little bit. You guys are doing a redo of the slides because they were actually slightly different on the video today than the ones we had seen before, which was fine. But I think we'll want to—

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Yes. So we're going to turn these around and give people an opportunity. We'll do one more turn of this, and then we'll have final slides agreed upon for the policy committee meeting, I believe on the 21st.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Yes, that's correct.

**Deven McGraw - Center for Democracy & Technology – Director**
Yes.

**Operator**
Excuse me, everyone. We have received a public comment.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Can that person please identify yourself, your name, and your organization?

**Operator**
Our question comes from Jeff Day from VNA.

**Jeff Day – VNA**
I just have a question. To what degree? It seems like – I just want to see, as I prepare to write a story. It seems that you went through the direct thing and got pretty far along in detailing that, and you were talking about putting this through with health information exchange. My impression is, things are a little bit more fluid there, and there may be substantial work done for your next draft in that area. Is that a fair assessment?

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
You know, I'm not sure I understand.

**Jeff Day – VNA**
Well, you seem to have gotten, in significant detail, gotten things nailed down when you're talking about the NHIN Direct in second half of this. There were somewhat, you know, more or less to be, you know, okay, let's rework this section. In the first half, you were dealing with the health information exchange going through health information exchange.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
I'm not sure this is the best forum.

**Jeff Day – VNA**
I didn't know when I was supposed to do it.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
But to clarify what we did today, the intention is that rather than immediately drilling down into whether there's going to be a certification program and what those organizations are going to be and do and functions, etc., was to put it within a much broader and hopefully comprehensive framework of what are the elements required to insure or at least improve or support public trust in any information exchange environment. That was the first part of the discussion was articulating it at a very high level a series of five.

**Jeff Day – VNA**
Yes. Got it.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Requirements for the trust framework. We then, having reached agreement on what those five meant in general, then did a little bit more of a more specific and concrete deep dive into the implications of that trust framework for the directed push use case of….

**Jeff Day – VNA**
Thank you for clarifying that.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Which is simplifying, so that's what we did today.

**Jeff Day – VNA**
Got it. It was much more specific, and I had noticed the difference.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Great.

**Jeff Day – VNA**
Thank you.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Thanks, everybody. We will turn around the slides, look forward to your additional comments and edits on those, and hopefully will be ready to go for the 21st.

**Judy Sparrow – Office of the National Coordinator – Executive Director**
Thank you.

**Deven McGraw - Center for Democracy & Technology – Director**
That's great.

**Farzad Mostashari – NYC DH&MHH – Assistant Commissioner**
Thanks, everybody.

**Deven McGraw - Center for Democracy & Technology – Director**
Thank you.

## Public Comment Received During the Meeting

1. The group may also want to consider genetic information and up-and-coming technologies which enable select parts of the genome to sequence. For example, should direct-to-consumer genetic companies (e.g. 23&Me) be regulated? After all, isn't ones DNA (because it is unique) a direct identifier?

2. What about the privacy and security of "de-identified" information sent/sold to data mining companies (e.g. IMS v. Ayotte)?